9-2019

Efficient oblivious transfer with membership verification

Weiwei LIU

Dazhi SUN

Yangguang TIAN
Singapore Management University, ygtian@smu.edu.sg

Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2019, Vol. 15(9)

DOI: 10.1177/1550147719875645
journals.sagepub.com/home/dsn
SAGE

Efficient oblivious transfer with membership verification

Weiwei Liu[1], Da-Zhi Sun[2] and Yangguang Tian[3]

Abstract

In this article, we introduce a new concept of oblivious transfer with membership verification that allows any legitimate group users to obtain services from a service provider in an oblivious manner. We present two oblivious transfer with membership verification schemes, differing in design. In the first scheme, a trusted group manager issues credentials for a pre-determined group of users so that the group of users with a valid group credential can obtain services from the service provider, while the choices made by group users remain oblivious to the service provider. The second scheme avoids the trusted group manager, which allows any user in the group to be a group manager, thus it is more suitable in distributed systems. In particular, we prove that the two oblivious transfer with membership verification schemes can achieve receiver's privacy and sender's privacy under a half-simulation model.

Keywords

Oblivious transfer, membership verification, trusted group manager, distributed systems

Date received: 28 December 2018; accepted: 5 August 2019

Handling Editor: José Camacho

Introduction

It is a well-known economic strategy that the service providers are usually willing to sell their goods or services to a group of users with a discount price to attract customers. The more people who make a batch buy, the better prices the service providers are willing to offer. In addition to a good price, the customer's privacy should be protected when buying goods or services from the service providers. With this motivation in mind, we aim to design oblivious transfer with membership verification schemes (MV-OT), which ensure that (1) user's privacy (e.g. consumption transcript) is hidden from the service provider, (2) only legitimate group users can obtain services from the service provider, and (3) the proposed MV-OT schemes should incur same computation and communication costs as conventional oblivious transfer with access control schemes.

To see whether MV-OT is useful in practice, we consider a scenario where an issuer (group manager) forms a group which includes certain number of users wanting to purchase digital goods or services from a service provider. After forming a group of users, the issuer first generates the group credential for all users. Next, the issuer registers the group with a service provider, who will verify whether the real number of users in the group is in accordance with the claimed number. After a successful authentication with the service provider, a valid group user can acquire the digital goods or services obliviously.

We stress that designing MV-OT schemes is a non-trivial task. The straightforward way to achieve MV-OT is to combine a broadcast encryption or a membership encryption scheme with a conventional oblivious

[1]School of Mathematics and Statistics, North China University of Water Resources and Electric Power, Zhengzhou, China
[2]College of Intelligence and Computing, Tianjin University, Tianjin, China
[3]School of Information Systems, Singapore Management University, Singapore

Corresponding author:
Yangguang Tian, School of Information Systems, Singapore Management University, 80 Stamford Road, Singapore 178902.
Email: ygtian@smu.edu.sg

transfer with access control scheme.[1,2] The group manager first encrypts the credential and broadcasts the ciphertext to every user in the group, only valid users in the group could obtain the credential, with which the users in the group could acquire services from a sender. However, there are several drawbacks in this straightforward combination. First, the combined algorithm inherits the computation and storage costs of two independent algorithms. Second, every user in the group has to share the same credential, which means if a dispute happens, even the group manager cannot decide which user should be accused. Third, a straightforward combination of two different algorithms may lead to new security issues.

Our contributions

We formulate the concept of MV-OT and present two concrete MV-OT schemes that can be applied in different applications. In the first scheme, a central authority first forms a group of users willing to make a batch buy from a service provider (or sender). The central authority generates credentials for group users and group token which is sent to the sender. The sender encrypts the digital contends with the group token to ensure only group users with valid credentials can acquire the digital goods or services successfully. The users outside the group cannot gain any information transmitted between the sender and the valid users in the group. In the second scheme, we remove the central authority to make it much more suitable in distributed applications. Any member in the group or even the sender can play the role of an issuer to generate group information.

It is worth noticing that the proposed schemes achieve privacy as well as membership verification without involving too much computation and communication costs. The comprehensive efficiency analysis of the proposed schemes shows that our proposed schemes just involve few extra computation and communication costs compared with the oblivious transfer with access control schemes in Han et al.,[1] which makes the proposed MV-OT schemes applicable in many distributed systems such as ad hoc mobile networks.

Related works

Oblivious transfer. Oblivious transfer has been applied widely in secure multiparty computation,[3] digital content browsing,[4] exchange of secrets[5] and other privacy-preserving systems.[1,2,6,7] Oblivious transfer has received much attention since it was first proposed by Rabin.[5] In the early works,[5,8] the sender can only one message $m_{b,\, b\in\{0,\,1\}}$ obliviously, which was soon extended to a more general k-out-of-n setting by Brassard et al.,[9] where a receiver could choose k messages obliviously from a sender. To ensure only legitimate receivers obtain contents from a receiver, Coull et al.[10] proposed an oblivious transfer scheme with access control using state graphs, where the receivers in the system can only acquire contents successfully from a sender if he has some unused states. Liu et al.[11] proposed the concept of traceable oblivious transfer such that the privacy of users is treated separately. The privacy of the honest receivers is well-protected while the privacy of the dishonest receivers could be traced by the sender.

Broadcast encryption. The concept of broadcast encryption was proposed by Fiat and Naor.[12] Broadcast encryption enables one broadcaster to transmit messages to a dynamically chosen group of users $\mathcal{S}$ such that $\mathcal{S} \subseteq \mathcal{N}$, where $\mathcal{N}$ refers to the set of all the users having access to the broadcast channel. Fiat and Naor[12] presented the first symmetric-key-based broadcast encryption scheme and the corresponding security model, which was extended to the public key setting by Dodis and Fazio.[13] Recently, Gritti et al.[14] proposed a novel broadcast encryption with dealership scheme which enables certain "dealers" in the broadcast system first to make a bulk buy from the broadcaster and then resell them in their own groups. Broadcast encryption with dealership accommodates a new business opportunity model and has received lots of attention.[15,16] Broadcast encryption can provide group membership verification; however, the "dealer" can trace the contents purchased by the users in the group, which in turn violates the privacy requirements in the aforementioned scenario.

Membership proof and membership encryption. Membership proof[17–20] is a very useful cryptographic primitive such that a user can prove to a verifier in a privacy-preserving manner that an attribute A belongs to a group G. Membership proof protocols can be further divided into two categories according to the information that can be accessed by the verifier. In the first category,[19,20] the verifier has knowledge of a token $\mathcal{P}(A)$ on a single attribute and all the attributes in $1G$. The prover can convince the verifier that $A \in \mathbf{G}$ without letting the verifier know which attribute it is in the group. In the second category,[17,18] the verifier has access to an attribute A and the group token $\mathcal{P}(\mathbf{G})$ containing information on a set of attributes. The prover can convince the verifier that $A \in \mathcal{P}(\mathbf{G})$ without leaking information of other attributes in the group. Membership encryption is proposed by Guo et al.[21,22] as a useful alternative primitive of membership proof. It employs the privacy-preserving group token $\mathcal{P}(\mathbf{G})$ in Au et al.[17] such that given $\mathcal{P}(\mathbf{G})$, it is computationally difficult to know the attributes or identities in $\mathcal{P}(\mathbf{G})$; however, a success decryption requires that a user holds the membership $A \in \mathbf{G}$.

Secret handshake. Secret handshake[23–25] is a useful primitive that can be applied in privacy-preserving applications where group membership verification is indispensable. The concept of secret handshake was introduced by Balfanz et al.,[23] which enables some entities in the same group to authenticate each other anonymously without leaking private information. Later on, Xu and Yung[24] proposed a secret handshake scheme achieving k-unlikability, which means an adversary can only infer that the participant is one out of the k users in the group. Recently, Tian et al.[25] proposed a k-time secret handshake scheme that allows valid users in a group to authenticate each other up to k times with a group credential. Otherwise, the private information can be traced in public. To achieve group membership verification, secret handshake schemes require that the service provider has to stay within the same group with all the users, which is impractical for the setting mentioned in the aforementioned scenario.

Article organization. The rest of the article is organized as follows. We introduce the formal definition and the security model of MV-OT in section "Security model." Some preliminaries are presented in section "Preliminaries," and concrete MV-OT schemes are presented in section "Our proposed schemes." We prove their security and analyze their efficiency in section "Security analysis," and the article is concluded in section "Conclusion."

Security model

In this section, we present the formal definition and the security model for MV-OT schemes.

Definition

There are three entities in an MV-OT system, namely, a receiver, a sender, and an issuer who behaves on behalf of a group manager. We assume there exists a public key infrastructure (PKI) that issues certificates on users' public keys. First, the issuer forms a group containing the users willing to obtain services from the sender. Then, the issuer generates the group token and sends it to the sender via a secure channel. The issuer generates credentials for each user in the group, with which the user (i.e. the receiver) could obtain services or digital goods from the sender. The system consists of four algorithms as follows:

1. *Setup*. Taking as input of a security parameter κ, the **Setup** algorithm outputs the system public parameters *params*

$$params \leftarrow \mathbf{Setup}(1^{\kappa})$$

2. *KeyGen*. Taking as input of the system parameters *params*, the **KeyGen** generates the public key pairs for the senders, receivers, and issuer, respectively, in the system

$$(pk_I, sk_I) \leftarrow \mathbf{KeyGen}(params)$$

3. *GroupGen*. Taking as input of the systems parameters *params*, pseudonyms of l users $A_1, A_2, \ldots, A_l$, and the private key of the issuer, it returns the credential for the receivers and group token for the sender

$$\sigma_i \leftarrow \mathbf{GroupGen}(sk_I, A_i; params), 1 \leqslant i \leqslant l$$
$$\mathcal{P}(\mathbf{G}) \leftarrow \mathbf{GroupGen}(sk_I, A_1, A_2, \ldots, A_l; params)$$

4. *Commitment*. Taking as input of the group token $\mathcal{P}(G)$ and the system parameter *params*, the **Commitment** algorithm outputs n ciphertexts

$$(c_1, c_2, \ldots, c_n) \leftarrow \mathbf{Commitment}(\mathcal{P}(\mathbf{G}), m_1, m_2, \ldots, m_n; params)$$

5. *Transfer*. The polynomial probabilistic time algorithm **Transfer** is an interactive algorithm between a receiver A_i ($\in \mathcal{R}$) and the sender $\mathcal{S}$. The result of this algorithm is that the receiver with pseudonym A_i obtains the intended message while the sender $\mathcal{S}$ records a transcript on A_i choice

$$R_{i_j} \leftarrow \mathbf{Transfer}_{\mathcal{R}}(c_{i_j}, \sigma_{i_j}; params)$$
$$E_{i_j} \leftarrow \mathbf{Transfer}_{\mathcal{S}}(R_{i_j}; params)$$
$$m_{i_j} \leftarrow \mathbf{Transfer}_{\mathcal{R}}(c_{i_j}, E_{i_j}; params)$$

6. *Correctness*. We require that for any security parameter $\kappa \in \mathbb{N}$, if $params \leftarrow \mathbf{Setup}(1^{\kappa})$, $(pk_I, sk_I) \leftarrow \mathbf{KeyGen}(params)$, $\sigma_i \leftarrow \mathbf{GroupGen}(sk_I, A_i; params)$, $1 \leqslant i \leqslant l$, $\mathcal{P}(\mathbf{G}) \leftarrow \mathbf{GroupGen}(sk_I, A_1, A_2, \ldots, A_l; params)$, $(c_1, c_2, \ldots, c_n) \leftarrow \mathbf{Commitment}(\mathcal{P}(\mathbf{G}), m_1, m_2, \ldots, m_n; params)$, $R_{i_j} \leftarrow \mathbf{Transfer}_{\mathcal{R}}(c_{i_j}, \sigma_{i_j}; params)$, and $E_{i_j} \leftarrow \mathbf{Transfer}_{\mathcal{S}}(R_{i_j}; params)$, then the receiver can obtain the intended message

$$m_{i_j} \leftarrow \mathbf{Transfer}_{\mathcal{R}}(c_{i_j}, E_{i_j}; params)$$

Security model

The security model presented in this section follows the half-simulation model in Naor and Pinkas.[26] We define that an MV-OT scheme is secure if the following conditions hold:

1. *Receiver's privacy*. The sender $\mathcal{S}$ cannot obtain any information about the receiver's choices. To be specific, for any two different choice sets

$\mathcal{C} = \{i_1, i_2, \ldots, i_k\}$ and $\mathcal{C}' = \{i_1', i_2', \ldots, i_k'\}$, the corresponding transcripts $\mathcal{B} = \{B_{i_1}, B_{i_2}, \ldots, B_{i_k}\}$ and $\mathcal{B}' = \{B_{i_1}', B_{i_2}', \ldots, B_{i_k}'\}$ are indistinguishable if the corresponding messages $\mathcal{M} = \{m_{i_1}, m_{i_2}, \ldots, m_{i_k}\}$ and $\mathcal{M}' = \{m_{i_1}', m_{i_2}', \ldots, m_{i_k}'\}$ are identically distributed.

2. *Sender's privacy*. A valid receiver $\mathcal{R}$ cannot obtain any information other messages $m_i, i \notin \{i_1, i_2, \ldots, i_k\}$ other than the intended contents. The security of the sender is defined through the real-world/ideal-world paradigm. In the real world, the sender and the receiver execute the protocols following the algorithm. In the ideal world, the protocol is executed with a trusted third party (TTP). The sender sends all the messages $m_1, m_2, \ldots, m_n$ to the TTP, where the receiver acquires the intended choices $m_{i_1}, m_{i_2}, \ldots, m_{i_k}$ adaptively. If $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$, then TTP sends $m_{i_1}, m_{i_2}, \ldots, m_{i_k}$ to the receiver. An MV-OT scheme is said to provide the privacy of the sender if for any receiver $\mathcal{R}$ in real world, there exists a probabilistic polynomial time (PPT) $\mathcal{R}'$ such that the outputs of $\mathcal{R}$ and $\mathcal{R}'$ are indistinguishable.
3. *Semantic security*. If a receiver $\mathcal{R}$ does not have a valid group credential $\sigma_i, 1 \leqslant i \leqslant l$, she cannot obtain any useful information $m_i, 1 \leqslant i \leqslant n$ from the sender $\mathcal{S}$.

Preliminaries

Bilinear pairing

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be multiplicative cyclic groups with prime order q. Let g and h be generators of $\mathbb{G}_1$. A bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfies the following conditions:

- Bilinearity: $e(g^a, h^b) = e(g, h)^{ab}$ for all $g, h \in \mathbb{G}_1$ and $a, b \in \mathbb{G}_q$.
- No-degeneracy: $e(g, h) \neq I_{\mathbb{G}_2}$, where $I_{\mathbb{G}_2}$ is the identity in $\mathbb{G}_2$.
- Computability: there is an efficient algorithm to compute $e(g, h)$ for all $g, h \in \mathbb{G}_1$.

Complexity assumptions

Definition 1. Discrete logarithm (DL) assumption. Let $\mathbb{G}$ be a cyclic group with a prime order q and g be a generator of $\mathbb{G}$. Given a random element $X \in \mathbb{G}$, compute $x \in \mathbb{Z}_p^*$ such that $X = g^x \bmod q$. Let $Adv_{\mathcal{A}}^{DL}(\kappa)$ be the advantage of a PPT adversary. We say that DL assumption holds in $\mathbb{G}$ that for all PPT adversary $\mathcal{A}$, the following function $Adv_{\mathcal{A}}^{DL}(\kappa)$ is negligible

$$Adv_{\mathcal{A}}^{DL}(\kappa) = Pr[(g^x = X, x \in \mathcal{Z}_q^*) \leftarrow \mathcal{A}(params, g, X, \mathbb{G})]$$

Definition 2. One-generator l-strong Diffie–Hellman (l-SDH) assumption.[27] Let $(\mathbb{G}_1, \mathbb{G}_2)$ be a bilinear group, for a randomly chosen element $x \in \mathcal{Z}_q^*$ and a random generator $g \in \mathbb{G}_1$, the l-SDH problem is, given $g, g^x, g^{x^2}, \ldots, g^{x^l} \in \mathbb{G}_1^{l+1}$, to compute a pair $(g^{1/(x+c)}, c)$. Define the advantage of a PPT adversary as $Adv_{\mathcal{A}}^{OG-l-SDH}(\kappa)$, and we say the l-SDH assumption holds if for all PPT algorithm $\mathcal{A}$, the following function $Adv_{\mathcal{A}}^{OG-l-SDH}(\kappa)$ is negligible

$$Adv_{\mathcal{A}}^{OG-l-SDH}(\kappa) = Pr[(g^{\frac{1}{x+c}}, c \in \mathcal{Z}_q^*) \leftarrow \mathcal{A}(params, g, g^x, \ldots, g^{x^l})]$$

Definition 3. Extended chosen-target computational Diffie–Hellman (XCT-CDH) assumption.[1] Let $\mathbb{G}$ be a cyclic group with prime order q and $x \in \mathcal{Z}_q^*$, there is a help oracle $H_{\mathbb{G}}(\cdot)$ that takes g_i as input and returns g_i^x. Given a $(k+1)$ tuple $\{g^{a_1}, g^{a_2}, \ldots, g^{a_{k+1}}\}$, where $a_i \in z_q^*$ for $i = 1, 2, \ldots, k+1$, define the advantage $Adv_{\mathcal{A}}^{XCT-CDH}(\kappa)$ of a PPT adversary $\mathcal{A}$, and XCT-CDH assumption holds in G, if for all PPT adversary $\mathcal{A}$ that $Adv_{\mathcal{A}}^{XCT-CDH}(\kappa)$ is negligible

$$Adv_{\mathcal{A}}^{XCT-CDH}(\kappa) = Pr[g^{xa_{k+1}} \leftarrow \mathcal{A}^{H_{\mathbb{G}}(\cdot)}(q, g, g^x, g^{a_{i_1}}, \ldots, g^{a_{i_k}})]$$

where $a_{i_j} \in \{a_1, a_2, \ldots, a_{k+1}\}$, for all $j = 1, 2, \ldots, k+1$.

Our proposed schemes

In this section, we present two MV-OT schemes. In the first scheme, there is an issuer generating credentials for the members in the group. Our construction takes advantage of the techniques of accumulator scheme in Nguyen.[18] In the first proposed scheme, the system parameters contain two secret keys (α, β) and some auxiliary parameters $g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^l}, g^{\beta}, g^{\beta\alpha}, g^{\beta\alpha^2}, \ldots, g^{\beta\alpha^l}$. While the group token is $\mathcal{P}(\mathbf{G}) = (\omega_1, \omega_2) = (g^{\tau \prod_{i=1}^{l} (\alpha + A_i)}, g^{\tau\beta \prod_{i=1}^{l} (\alpha + A_i)})$, the membership verification process is described as follows:

1. If user A_i is a valid group user with credential $\sigma_{A_i} = g^{\frac{1}{(\alpha + A_i)(\beta + A_i)}}$, then it would be computationally easy to recover

$$e((\omega_2 \omega_1^{A_i})^{t_j}, g^{\frac{1}{(\alpha + A_i)(\beta + A_i)}}) = e(g, g)^{\tau t_j \prod_{A_j \in A/A_i} (\alpha + A_j)}$$

which is further used to extract the intended message.

2. Otherwise, if a dishonest user A_k who does not belong to the group tries to interact with the sender, we have

$$e((\omega_2\omega_1^{A_k})^{t_j}, g^{\frac{1}{(\alpha+A_k)(\beta+A_k)}}) = e(g,g)^{\tau t_j \frac{\prod_{j=1}^{j=l}(\alpha+A_j)}{\alpha+A_k}}$$

which contains the inversion exponent $g^{1/(\alpha+A_k)}$ that is computationally infeasible to be computed from the system parameters.

MV-OT $^{n}_{k\times 1}$-I

The proposed scheme consists of a tuple of PPT algorithms as follows:

1. *Setup*. Taking as input a security parameter κ, this algorithm outputs a bilinear group $(e, \mathbb{G}_1, \mathbb{G}_2)$ where $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ and $\mathbb{G}_1, \mathbb{G}_2$ are cyclic groups with prime q. Let g be a generator of $\mathbb{G}_1$. The system parameters $params = (e, \mathbb{G}_1, \mathbb{G}_2, q, g)$.
2. *KeyGen*. Suppose there are l users with pseudonyms $A_1, A_2, \ldots, A_l$ in the group, the issuer (i.e. group manager) chooses $\alpha, \beta \in \mathbb{Z}_q^*$ and computes $g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^l}, g^{\beta}, g^{\beta\alpha}, g^{\beta\alpha^2}, \ldots, g^{\beta\alpha^l}$ and generates the group token $\mathcal{P}(\mathbf{G}) = (\omega_1, \omega_2) = (g^{\tau\prod_{i=1}^{l}(\alpha+A_i)}, g^{\tau\beta\prod_{i=1}^{l}(\alpha+A_i)})$, where $\tau \in \mathbb{Z}_q^*$ is chosen at random by the issuer. For each user with pseudonym $A_i, 1 \leqslant i \leqslant l$, the issuer computes $\sigma_{A_i} = g^{1/((\alpha+A_i)(\beta+A_i))}$ and returns it to the individual users. I sends $(\mathcal{P}(\mathbf{G}), \alpha)$ to the sender $\mathcal{S}$.
3. *Commitment*. in response to the requirement from a user with pseudonym A_i, $\mathcal{S}$ chooses n different random elements $t_1, t_2, \ldots, t_n \in \mathbb{Z}_q^*$ and a one-time secret $z \in \mathbb{Z}_q^*$, $\mathcal{S}$ computes the ciphertext of $m_1, m_2, \ldots, m_n$ as $c_j = (c_{j,1}, c_{j,2})$ where $c_{j,1} = (\omega_2\omega_1^{A_i})^{t_j}$ and $c_{j,2} = e(\omega_1, g)^{\frac{z\cdot t_j}{\alpha+A_i}} = e(g,g)^{\tau z t_j \prod_{A_j \in A/A_i}(\alpha+A_j)} \cdot m_j$, $\mathcal{S}$ sends $c_1, c_2, \ldots, c_n$ to A_i.
4. *Transfer*. Upon receiving the ciphertexts from the sender, the receiver with pseudonym A_i chooses $r_i \in \mathbb{Z}_q^*$ and computes $B_{i_j} = e(c_{i_j,1}, \sigma_{A_i})$, $E_{i_j} = e(c_{i_j,1}, \sigma_{A_i})^{r_i}$, where $i_j \in \{1, 2, \ldots, n\}$, then the receiver A_i sends E_{i_j} to $\mathcal{S}$. $\mathcal{S}$ computes $D_{i_j} = (E_{i_j})^{z}$ and sends it to $\mathcal{R}$. $\mathcal{R}$ computes $K_{i_j} = D_{i_j}^{r_i^{-1}}$ and obtains the intended message $m_{i_j} = c_{i_j,2}/K_{i_j}$.

Correctness. Suppose the receiver with pseudonym A_i is a valid group member with credential σ_{A_i}. The correctness check of MV-OT $^{n}_{k\times 1}$-II scheme is as follows

$$\begin{aligned} E_{i_j} &= e(c_{i_j,1}, \sigma_{A_i})^{r_i} \\ &= e((\omega_2\omega_1^{A_i})^{t_{i_j}}, g^{\frac{1}{(\beta+A_i)(\alpha+A_i)}})^{r_i} \\ &= e(g^{\tau t_{i_j}(\beta+A_i)\prod_{j=1}^{m}(\alpha+A_j)}, g^{\frac{1}{(\beta+A_i)(\alpha+A_i)}})^{r_i} \\ &= e(g,g)^{r_i\tau t_{i_j}\prod_{A_j\in A/A_i}(\alpha+A_j)} \end{aligned}$$

and

$$\begin{aligned} \frac{c_{i_j,2}}{K_{i_j}} &= \frac{e(g,g)^{\tau z t_{i_j}\prod_{A_j\in A/A_i}(\alpha+A_j)} \cdot m_{i_j}}{D_{i_j}^{r_i^{-1}}} \\ &= \frac{e(g,g)^{\tau z t_{i_j}\prod_{A_j\in A/A_i}(\alpha+A_j)} \cdot m_{i_j}}{E_{i_j}^{zr_i^{-1}}} \\ &= \frac{e(g,g)^{\tau z t_{i_j}\prod_{A_j\in A/A_i}(\alpha+A_j)} \cdot m_{i_j}}{e(g,g)^{\tau z t_{i_j}\prod_{A_j\in A/A_i}(\alpha+A_j)}} \\ &= m_{i_j} \end{aligned}$$

MV-OT $^{n}_{k\times 1}$-II

In the MV-OT $^{n}_{k\times 1}$-I scheme, it involves a central authority named issuer helps to form and maintain the group, which makes it unpractical in distributed scenarios. Therefore, we proposed the second scheme MV-OT $^{n}_{k\times 1}$-II without a central authority. Anyone who tries to make a batch buy or even the sender could behave as the group manager to initialize the system. The proposed MV-OT $^{n}_{k\times 1}$-II scheme consists of a tuple of PPT algorithms as follows:

1. *Setup*. Taking as input a security parameter κ, this algorithm outputs a bilinear group $(e, \mathbb{G}_1, \mathbb{G}_2)$ where $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ and $\mathbb{G}_1, \mathbb{G}_2$ are cyclic groups with prime q. Let g and h be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. The system parameters $params = (e, \mathbb{G}_1, \mathbb{G}_2, q, g, h)$.
2. *KeyGen*. Suppose there is an initial setup phase and there have been l users with pseudonyms $A_1, A_2, \ldots, A_l$ in the group. The sender chooses $\alpha \in \mathbb{Z}_q^*$ and computes $g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^l}$ and generates the group token $\mathcal{P}(\mathbf{G}) = g^{\tau\prod_{i=1}^{l}(\alpha+A_i)}$, where $\tau \in \mathbb{Z}_q^*$ is randomly chosen by the sender. For each user with pseudonym $A_i, 1 \leqslant i \leqslant m$, the sender computes and returns $\sigma_{A_i} = g^{1/(\alpha+A_i)}$.
3. *Commitment*. In response to the requirement from a user with pseudonym A_i. $\mathcal{S}$ chooses n different random numbers $t_1, t_2, \ldots, t_n \in \mathbb{Z}_q^*$ and a one-time secret $z \in \mathbb{Z}_q^*$. $\mathcal{S}$ computes the ciphertext of $m_1, m_2, \ldots, m_n$ as $c_i = (c_{i,1}, c_{i,2})$ where $c_{i,1} = g^{\tau t_i\prod_{j=1}^{m}(\alpha+A_j)}$ and $c_{i,2} =$

$e(g,g)^{\tau z t_i \prod_{A_j \in A/A_i}(\alpha + A_j)} \cdot m_i$. $\mathcal{S}$ sends $c_1, c_2, \ldots, c_n$ to A_i.

4. *Transfer*. Upon receiving ciphertexts from the sender, A_i chooses $r_i \in \mathbb{Z}_q^*$ and computes $B_{i_j} = e(c_{i_j}, \sigma_{A_i})$ and $E_{i_j} = B_{i_j}^{r_i}$, where i_j is the index of message of the receiver's choice and $i_j \in \{1, 2, \ldots, n\}$, then the receiver A_i sends E_{i_j} to $\mathcal{S}$. $\mathcal{S}$ computes $D_{i_j} = (E_{i_j})^z$ and sends it to $\mathcal{R}$. $\mathcal{R}$ computes $K_{i_j} = D_{i_j}^{r_i^{-1}}$ and obtains the intended message $m_{i_j} = c_{i_j,2}/K_{i_j}$.

Correctness. Suppose the receiver with pseudonym A_i is valid group member with credential σ_{A_i}. The correctness check of MV-OT $\binom{n}{k \times 1}$-II scheme is as follows

$$\begin{aligned} E_{i_j} &= e(c_{i_j,1}, \sigma_{A_i})^{r_i} \\ &= e\left(g^{\tau t_{i_j} \prod_{j=1}^{m}(\alpha + A_j)}, g^{\frac{1}{\alpha + A_i}}\right)^{r_i} \\ &= e(g,g)^{r_i \tau t_{i_j} \prod_{A_j \in A/A_i}(\alpha + A_j)} \end{aligned}$$

and

$$\begin{aligned} \frac{c_{i_j,2}}{K_{i_j}} &= \frac{e(g,g)^{\tau z t_{i_j} \prod_{A_j \in A/A_i}(\alpha + A_j)} \cdot m_{i_j}}{D_{i_j}^{r_i^{-1}}} \\ &= \frac{e(g,g)^{\tau z t_{i_j} \prod_{A_j \in A/A_i}(\alpha + A_j)} \cdot m_{i_j}}{E_{i_j}^{z r_i^{-1}}} \\ &= \frac{e(g,g)^{\tau z t_{i_j} \prod_{A_j \in A/A_i}(\alpha + A_j)} \cdot m_{i_j}}{e(g,g)^{\tau z t_{i_j} \prod_{A_j \in A/A_i}(\alpha + A_j)}} \\ &= m_{i_j} \end{aligned}$$

Security analysis

Security analysis

The security result of our MV-OT schemes is shown by the following theorems.

Theorem 1. The proposed MV-OT $\binom{n}{k \times 1}$-I scheme provides receiver's privacy for honest receivers.

Proof. Suppose an honest receiver with pseudonym A_i requests contents from the sender. $\{E_{i_1}, E_{i_2}, \ldots, E_{i_k}\}$ is a set of transcripts on A_i choices. For any E_{i_j} such that $j \in \{1, 2, \ldots, k\}$, $E_{i_j} = e(g,g)^{r_i t_{i_j} \tau \prod_{A_j \in A/A_i}(\alpha + A_j)}$. Set $W_i = e(g,g)^{\tau \prod_{A_j \in A/A_i}(\alpha + A_j)} \in \mathbb{G}_2$, then there exits $r_i' \in \mathbb{Z}_q^*$ such that $E_{i_j} = W_i^{r_i t_{i_j}} = W_i^{r_i' t_{i_w}}$, where $t_{i_w} \neq t_{i_j}$ and $t_{i_w} \in \{t_1, t_2, \ldots, t_n\}$, which means the choice of the receiver is computationally indistinguishable to the sender as long as the DL problem is hard in $\mathbb{G}_2$.

Theorem 2. The proposed MV-OT $\binom{n}{k \times 1}$-I scheme provides sender's privacy.

Proof. Suppose an honest receiver runs the MV-OT protocol with the sender $\mathcal{S}$ to obtain k messages. For any PPT malicious receiver $\hat{\mathcal{R}}$ in the real world, we are able to construct a PPT malicious receiver $\hat{\mathcal{R}}^*$ in the ideal model such that the outputs of $\hat{\mathcal{R}}$ and $\hat{\mathcal{R}}^*$ are indistinguishable. $\hat{\mathcal{R}}^*$ simulates the honest sender $\mathcal{S}$ in the real world and interacts with $\hat{\mathcal{R}}$ as follows:

1. $\mathcal{S}$ sends the messages $m_1, m_2, \ldots, m_n$ to the *TTP*.
2. $\hat{\mathcal{R}}^*$ sends $c_1^*, c_2^*, \ldots, c_n^*$ to *TTP* such that $c_i^* = (c_{i_1}, c_{i_2}) \in \mathbb{G}_1 \times \mathbb{G}_2$ for $i = 1, 2, \ldots, n$, where $c_1^*, c_2^*, \ldots, c_n^*$ are n different pairs of random numbers selected from $\mathbb{G}_1$ and $\mathbb{G}_2$ by $\hat{\mathcal{R}}^*$.
3. $\hat{\mathcal{R}}^*$ monitors the outputs of $\hat{\mathcal{R}}^*$, if $\hat{\mathcal{R}}$ can compute $B_{i_1}, B_{i_2}, \ldots, B_{i_k}$ and $E_{i_1}, E_{i_2}, \ldots, E_{i_k}$. $\hat{\mathcal{R}}^*$ chooses random $B_{i_1}^*, B_{i_2}^*, \ldots, B_{i_k}^* \in \mathbb{G}_2$ and $E_{i_1}^*, E_{i_2}^*, \ldots, E_{i_k}^* \in \mathbb{G}_2$.
4. When $\hat{\mathcal{R}}$ requires $D_{i_1}, D_{i_2}, \ldots, D_{i_k}$ from $E_{i_1}, E_{i_2}, \ldots, E_{i_k}$, $\hat{\mathcal{R}}^*$ queries the help oracle $H_{\mathbb{G}_2}(\cdot)$ on $E_{i_1}^*, E_{i_2}^*, \ldots, E_{i_k}^*$ and gets back $D_{i_1}^*, D_{i_2}^*, \ldots, D_{i_k}^*$, where $D_{i_j}^* = (E_{i_j}^{z^*})$, $j = 1, 2, \ldots, k$.
5. If $\hat{\mathcal{R}}$ can compute $K_{i_j} = e(g,g)^{\tau z t_{i_j} \prod_{A_j \in A/A_i}(\alpha + A_j)}$, $\hat{\mathcal{R}}^*$ sends i_j to *TTP*, *TTP* returns $K_{i_j}^* = c_{i_j,2}^*/m_{i_j}$.
6. $\hat{\mathcal{R}}^*$ outputs $(B_{i_1}^*, B_{i_2}^*, \ldots, B_{i_k}^*, E_{i_1}^*, E_{i_2}^*, \ldots, E_{i_k}^*, c_1^*, c_2^*, \ldots, c_n^*)$.

In the simulation process, if $\hat{\mathcal{R}}$ obtains $k+1$ messages while $\hat{\mathcal{R}}^*$ is unaware of the indices of the corresponding messages, the simulation aborts. Otherwise, we are able to show that $\hat{\mathcal{R}}$ is only able to choose at most k messages under the XCT-CDH assumption. If $\hat{\mathcal{R}}$ can get $k+1$ messages, he can compute E_{i_j} for $j = 1, 2, \ldots, k+1$. That is, if $\hat{\mathcal{R}}$ can obtain

$$(e(g,g)^{\tau t_{i_1} \prod_{A_j \in A/A_i}(\alpha + A_j)})^z, (e(g,g)^{\tau t_{i_2} \prod_{A_j \in A/A_i}(\alpha + A_j)})^z, \ldots, (e(g,g)^{\tau t_{i_k} \prod_{A_j \in A/A_i}(\alpha + A_j)})^z$$

$\hat{\mathcal{R}}$ can compute

$$(e(g,g)^{\tau t_{i_{k+1}} \prod_{A_j \in A/A_i}(\alpha + A_j)})^z$$

which contradicts the XCT-CDH assumption. Therefore, $\hat{\mathcal{R}}$ can only obtain the required messages from the sender and cannot obtain any information on other messages that he hasn't required.

We can see from Theorem 1 that $\{B_{i_1}, B_{i_2}, \ldots, B_{i_k}\}$ and $\{E_{i_1}, E_{i_2}, \ldots, E_{i_k}\}$ are indistinguishable from random elements in $\mathbb{G}_2$ and $\{c_1, c_2, \ldots, c_n\}$ are indistinguishable from random elements in $\mathbb{G}_1 \times \mathbb{G}_2$ by Theorem 3. In addition, the sets of $\{D_{i_1}, D_{i_2}, \ldots, D_{i_k}\}$

Table 1. Computational costs of the proposed schemes.

Algorithm	KeyGen	Commitment	Transfer
MV-OT $^{n}_{k\times 1}$-I	$(3l+2)E_{\mathbb{G}_1}$	$n(E_{\mathbb{G}_1}+E_{\mathbb{G}_2})$	$kP+4kE_{\mathbb{G}_2}$
MV-OT $^{n}_{k\times 1}$-II	$(2l+1)E_{\mathbb{G}_1}$	$n(E_{\mathbb{G}_1}+E_{\mathbb{G}_2})$	$kP+4kE_{\mathbb{G}_2}$

Table 2. Communication costs of the proposed schemes.

Algorithm	KeyGen	Commitment	Transfer
MV-OT $^{n}_{k\times 1}$-I	$(l+2)\mathbb{G}_1$	$n\mathbb{G}_1+n\mathbb{G}_2$	$2k\mathbb{G}_2$
MV-OT $^{n}_{k\times 1}$-II	$l\mathbb{G}_1$	$n\mathbb{G}_1+n\mathbb{G}_2$	$2k\mathbb{G}_2$

and $\{D^*_{i_1}, D^*_{i_2}, \ldots, D^*_{i_k}\}$ are identically distributed. Therefore, no distinguishers can distinguish the outputs of $\hat{\mathcal{R}}$ and $\hat{\mathcal{R}}'$ with a non-negligible probability.

Theorem 3. The proposed MV-OT $^{n}_{k\times 1}$ scheme is semantic secure.

Proof. The semantic security of MV-OT $^{n}_{k\times 1}$-I is analyzed through two aspects. First, if the adversary $\mathcal{A}$ could forge $\sigma_{A_i} = g^{1/((\beta+A_i)(\alpha+A_i))}$, then $\mathcal{A}$ could act as authorized receiver to communicate with the sender. In this case, there exists another PPT algorithm $\mathcal{B}$ that could use $\mathcal{A}$ to break l-SDH assumption. Second, if the adversary $\mathcal{A}$ could compute $e(g,g)^{\tau z t_i \prod_{A_j \in A/A_i}(\alpha+A_j)}$ from the ciphertext $c_i = (c_{i,1}, c_{i,2})$, then $\mathcal{A}$ could also obtain messages from the receiver. In this case, there exists a PPT algorithm that could take advantage of $\mathcal{A}$ to break the XCT-CDH assumption. Therefore, MV-OT $^{n}_{k\times 1}$-I is semantically secure.

Theorem 4. The proposed MV-OT $^{n}_{k\times 1}$-II scheme provides receiver's privacy for honest receivers. The security proof and the subsequent proofs of the MV-OT $^{n}_{k\times 1}$-II scheme are similar as that for MV-OT $^{n}_{k\times 1}$-I, thus we omit it.

Theorem 5. The proposed MV-OT $^{n}_{k\times 1}$-II scheme provides sender's privacy.

Theorem 6. The proposed MV-OT $^{n}_{k\times 1}$-II scheme is semantic secure.

Efficiency analysis

We present a comprehensive complexity analysis in terms of computation and communication costs. The results are presented in Tables 1 and 2, respectively. By l, n, and k, we denote the number of users in the group, the total number of the messages, and the number of messages selected by a receiver. Let $E_{\mathbb{G}_1}$ and $E_{\mathbb{G}_2}$ denote the exponential operations in $\mathbb{G}_1$ and $\mathbb{G}_2$, and P one pairing operation.

Conclusion

In this article, we formulate the concept of MV-OT such that only legitimate users with proper membership can obliviously acquire digital goods or services from a service provider. We have proposed two MV-OT schemes with completed security analysis. The two MV-OT schemes are different in design, and the one without trusted group manager is preferable in distributed systems.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was partially sponsored by the National Science Foundation of China under grant no. 61872264.

ORCID iD

Weiwei Liu https://orcid.org/0000-0002-3986-8347
Yangguang Tian https://orcid.org/0000-0002-6624-5380

References

1. Han J, Susilo W, Mu Y, et al. Efficient oblivious transfers with access control. *Comput Math Appl* 2012; 63(4): 827–837.
2. Han J, Susilo W, Mu Y, et al. AAC-OT: accountable oblivious transfer with access control. *IEEE T Inf Foren Sec* 2015; 10(12): 2502–2514.
3. Yao AC. Protocols for secure computations (extended abstract). In: *23rd annual symposium on foundations of computer science*, Chicago, IL, 3–5 November 1982, pp.160–164. New York: IEEE.
4. Liu W, Mu Y, Yang G, et al. Efficient e-coupon systems with strong user privacy. *Telecommun Syst* 2017; 64(4): 695–708.

5. Rabin M. How to exchange secrets with oblivious transfer. Technical report, Aiken Computation Laboratory, Harvard University, 20 May 1981.
6. Aiello B, Ishai Y and Reingold O. Priced oblivious transfer: how to sell digital goods. In: *International conference on the theory and application of cryptographic techniques: advances in cryptology*, 2001, pp.119–135, https://www.iacr.org/archive/eurocrypt2001/20450118.pdf
7. Guo F, Mu Y, Susilo W, et al. Privacy-preserving mutual authentication in RFID with designated readers. *Wireless Pers Commun* 2017; 96(3): 4819–4845.
8. Even S, Goldreich O and Lempel A. A randomized protocol for signing contracts. *Commun ACM* 1985; 28(6): 637–647.
9. Brassard G, Crépeau C and Robert J. All-or-nothing disclosure of secrets. In: *Advances in cryptology—CRYPTO '86*, Santa Barbara, CA, 1 January 1987, pp.234–238. Berlin: Springer.
10. Coull SE, Green M and Hohenberger S. Controlling access to an oblivious database using stateful anonymous credentials. In: *Public key cryptography—PKC 2009*, Irvine, CA, 18–20 March 2009, pp.501–520. Berlin: Springer.
11. Liu W, Zhang Y, Mu Y, et al. Efficient traceable oblivious transfer and its applications. In: *14th international conference on information security practice and experience, ISPEC 2018*, Tokyo, Japan, 25–27 September 2018, pp.610–621. Berlin: Springer.
12. Fiat A and Naor M. Broadcast encryption. In: *13th annual international cryptology conference on advances in cryptology—CRYPTO '93*, Santa Barbara, CA, 22–26 August 1993, pp.480–491. Berlin: Springer.
13. Dodis Y and Fazio N. Public key trace and revoke scheme secure against adaptive chosen ciphertext attack. In: *6th international workshop on theory and practice in public key cryptography—PKC 2003*, Miami, FL, 6–8 January 2003, pp.100–115. Berlin: Springer.
14. Gritti C, Susilo W, Plantard T, et al. Broadcast encryption with dealership. *Int J Inf Sec* 2016; 15(3): 271–283.
15. Acharya K and Dutta R. Adaptively secure broadcast encryption with dealership. In: *19th international conference on information security and cryptology—ICISC 2016, revised selected papers*, Seoul, South Korea, 30 November–2 December 2016, pp.161–177. Berlin: Springer.
16. Kim JS, Lee YK, Eom J, et al. Recipient revocable broadcast encryption with dealership. In: *20th international conference on information security and cryptology—ICISC 2017, revised selected papers*, Seoul, South Korea, 29 November–1 December 2017, pp.214–228. Berlin: Springer.
17. Au MH, Tsang PP, Susilo W, et al. Dynamic universal accumulators for DDH groups and their application to attribute-based anonymous credential systems. In: *Cryptographers' track at the RSA conference 2009: topics in cryptology—CT-RSA 2009*, San Francisco, CA, 20–24 April 2009, pp.295–308. Berlin: Springer.
18. Nguyen L. Accumulators from bilinear pairings and applications. In: *Cryptographers' track at the RSA conference 2005: topics in cryptology—CT-RSA 2005*, San Francisco, CA, 14–18 February 2005, pp.275–292. Berlin: Springer.
19. Camenisch J, Chaabouni R and Shelat A. Efficient protocols for set membership and range proofs. In: *14th international conference on the theory and application of cryptology and information security on advances in cryptology—ASIACRYPT 2008*, Melbourne, VIC, Australia, 7–11 December 2008, pp.234–252. Berlin: Springer.
20. Camenisch J and Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials. In: *22nd annual international cryptology conference on advances in cryptology—CRYPTO 2002*, Santa Barbara, CA, 18–22 August 2002, pp.61–76, http://groups.csail.mit.edu/cis/pubs/lysyanskaya/cl02a.pdf
21. Guo F, Mu Y, Susilo W, et al. Membership encryption and its applications. In: *18th Australasian conference on information security and privacy, ACISP 2013*, Brisbane, QLD, Australia, 1–3 July 2013, pp.219–234. Berlin: Springer.
22. Guo F, Mu Y and Susilo W. Subset membership encryption and its applications to oblivious transfer. *IEEE T Inf Foren Sec* 2014; 9(7): 1098–1107.
23. Balfanz D, Durfee G, Shankar N, et al. Secret handshakes from pairing-based key agreements. In: *2003 IEEE symposium on security and privacy (S&P 2003)*, Berkeley, CA, 11–14 May 2003, pp.180–196. New York: IEEE.
24. Xu S and Yung M. k-anonymous secret handshakes with reusable credentials. In: *Proceedings of the 11th ACM conference on computer and communications security, CCS 2004*, Washington, DC, 25–29 October 2004, pp.158–167. New York: ACM.
25. Tian Y, Zhang S, Yang G, et al. Privacy-preserving k-time authenticated secret handshakes. In: *22nd Australasian conference on information security and privacy, ACISP 2017, part II*, Auckland, New Zealand, 3–5 July 2017, pp.281–300. Berlin: Springer.
26. Naor M and Pinkas B. Computationally secure oblivious transfer. *J Cryptology* 2005; 18(1): 1–35.
27. Tanaka N and Saito T. On the q-strong Diffie–Hellman problem, 2010, https://eprint.iacr.org/2010/215.pdf